REMARKS/ARGUMENTS

These remarks are submitted in response to the Office Action dated February 10, 2009 (Office Action). As this response is timely filed within the 3-month shortened statutory period, no fee is believed due. However, the Examiner is expressly authorized to charge any deficiencies to Deposit Account No. 14-1437.

Claim Rejections – 35 USC § 103

Claims 1-4, 6-9, 15-17, and 19-21 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,664,109 to Johnson, *et al.* (hereinafter Johnson) in view of U.S. Patent 5,801,697 to Parikh, *et al.* (hereinafter Parikh). Claims 5, 10, 18, and 22 were rejected under 35 U.S.C. 103(a) as being unpatentable over Johnson in view of Parikh, and in further view of Official Notice. Claims 11-13 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Published Patent Application 2002/0022973 to Sun, *et al.* (hereinafter Sun) in view of Parikh. Claim 14 was rejected under 35 U.S.C. 103(a) as being unpatentable over Sun in view of Parikh, and in further view of U.S. Patent 5,897,493 to Brown (hereinafter Brown).

Although Applicant respectfully disagrees with the rejections, Applicants has amended independent Claims 1, 11, and 15 to even more clearly define the present invention and facilitate prosecution of the instant application. Applicant has cancelled Claims 5-10 and 18-22. However, Applicant is not conceding that the remaining claims as originally formulated or the cancelled claims fail to present patentable subject matter. The amendments and cancellations are solely for the purpose of expediting prosecution. Accordingly, neither the amendments nor cancellations should be interpreted as the surrender of any subject matter. Applicants expressly reserve the right to present the original version of any of the amended claims in any future divisional or continuation applications from the present application. As discussed herein, the claim amendments are fully supported throughout the Specification. No new matter has been introduced by the claim amendments.

Aspects of Applicants' Invention

It may be helpful to reiterate certain aspects of Applicants' invention prior to addressing the cited references. One embodiment of the invention, as typified by Claim 1, is a method for concealing displayed confidential information.

The method can include providing at least one publically accessible display and at least one private display; receiving confidential information from an input device connected to the publically accessible display; displaying at least a portion of the confidential information at the private display; and displaying at least a portion of the confidential information at the publically accessible display for a predetermined time period. The publically accessible display is configured to display the confidential information to only a view from within a predetermined viewing angle and a predetermined distance to the publically accessible display.

The method further can include concealing the portion of the confidential information displayed at the publically accessible display upon expiration of the predetermined time period or upon a user quest. The concealing step includes at least one of removing the confidential information from the publically accessible display, covering the confidential information, and presenting the information in a nonsensical format.

See, e.g., Specification, paragraphs [0021]-[0022] and [0038]-[0047].

The Claims Define Over The Prior Art

The ability to provide the appropriate health care to an individual can depend on the health care provider having access to information regarding the patient, particularly including the patient's medical history. Recent advances in digital technologies have enabled health care systems and providers to store vast amounts of information regarding the patient's medical history. This information, in most cases, can be accessed almost instantaneously by health care providers. Additionally, communication networks can enable confidential information to be updated in a central location so that updated information can be accessed from a multitude of remote locations. Thus, the digital revolution and the advances in communication technology have laid the foundation for an infrastructure that gives health care providers access to updated confidential information. See Specification, paragraph [0002].

While access to such information can greatly enhance the quality of health care provided to a patient, the amount of personal and confidential information available has caused concern regarding the confidentiality of the patient's private medical information. In reaction to a public outcry for the protection of health care information, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Thereafter, the "Privacy Rule" was adopted to elaborate on national standards for safeguards to protect the confidentiality, integrity, and availability of electronically protected health information. The Privacy Rule protects all individually identifiable health information that is held or transmitted by a health care provider. Individually identifiable health information can be information, including demographic data, that relates to the individual's past, present or future physical or mental health or condition, and that identifies the individual or can be used to identify the individual, such as the patient's name, address, birth date, and Social Security Number. See Specification, paragraph [0003].

While health care providers need to protect confidential information in order to comply with the Privacy Rule, the logistics of protecting confidential information must balance the protection of confidential information with the need of health care providers to have access to such information. Because many customary health care communications and practices play an important or even essential role in ensuring that individuals receive prompt and effective health care, such a balance must be delicately struck. See Specification, paragraph [0005].

Additionally, present health care systems involve a great number of people to provide not only comprehensive health care to a patient, but also to ensure that patients are appropriately billed. Many of these persons do not need to know an individual's private health care information. For example, while a hospital helper may need to know to push the wheelchair of a patient to operating room A so that the patient can have surgery, the hospital helper does not need to know why the patient is having surgery. In stark contrast, it is apparent that a complete medical history should be readily available to the surgeon. Thus, individuals involved in a patient's health care may not need the same amount of access to the patient health care information. See Specification, paragraph [0006].

Moreover, due to the nature of the communications and practices of the health care industry, as well as the various environments in which individuals receive health care, the measures incorporated should attempt to eliminate incidental disclosure of confidential information. For example, in a typical emergency room and/or waiting room, one patient may overhear a health care provider's confidential conversation with a patient, or may inadvertently glimpse at an emergency room sign-in sheet that likely contains the patient's name and reason for visiting the emergency room. While such communications may be necessary, health care providers now have a duty to place reasonable safeguards over the unnecessary dissemination of confidential patient information. See Specification, paragraph [0007].

The present invention provides a solution for ensuring confidential and private information remains undisclosed to unintended parties when such information is provided in a generally unsecured environment. More particularly, the present invention provides a system and method that allow an individual to provide confidential information to a publicly accessible device in which the confidential information is temporarily displayed. Moreover, the system and method allow the appropriate personnel to view the confidential information while preventing unauthorized personnel from accessing the information.

The invention provides a method and a system for concealing displayed confidential information. The method for concealing displayed confidential information includes providing at least one publically accessible display and at least one private display. The method also includes receiving confidential information from an input device connected to the publically accessible display, displaying at least a portion of the confidential information at the private display, and displaying at least a portion of the confidential information at the publically accessible display for a predetermined time period. For instance, the publically accessible display can display any information that is entered for only 5 seconds, 10 seconds, 15 seconds, 20 seconds, and so on. See Specification, paragraph [0019]. The publically accessible display is configured to display the confidential information to only a direct view from within a predetermined distance to the publically accessible display. In this way, the publically accessible display will not legibly display confidential information to a party with a view point at distance from or to the side of the publically accessible display. See Specification, paragraph [0022]. The method further includes concealing the portion of the confidential information displayed at the publically accessible display upon expiration of the predetermined time period or upon a user quest. The concealing step includes at least one of removing the confidential information from the publically accessible display, covering the confidential information, and presenting the information in a nonsensical format.

Johnson discloses a centralized record keeping system that receives record documents from one of a plurality of independent service providers. The system automatically links the record to a person who is the subject of the record by automatically extracting from the record demographic data on the subject and matching it to demographic data on the subject maintained in a database. Unique subject identifiers are not preassigned by the central record keeping system or used for linking. The records are stored in a repository and a list of linked records is maintained for each person. All records for a particular subject are then available for retrieval by querying the database of demographic data. See col. 2, lines 14-26.

Clearly, Johnson concerns a method of extracting a pre-defined data item from unstructured medical service records stored in a central data processing system and generated by a plurality of service providers. In contrast, the present invention concerns concealing confidential information displayed at a publically accessible display. The subject matter of Johnson thus has nothing to do with the subject matter of the present invention.

More particularly, Johnson at least does not disclose receiving confidential information from an input device connected to a publically accessible display; displaying at least a portion of the confidential information at a publically accessible display, which is configured to display the confidential information to only a view from within a predetermined viewing angle and a predetermined distance to the publically accessible display, for a predetermined time period; and concealing the portion of the confidential information displayed at the publically accessible display upon expiration of the predetermined time period or upon a user quest by at least one of removing the confidential information from the publically accessible display, covering the confidential information, and presenting the information in a nonsensical format, as in the clamed invention.

Parikh does not make up for the deficiencies of Johnson.

Parikh discloses a method of reducing a likelihood of unauthorized observation of on-screen computer data by dividing the computer screen work area into a visible area and an obscured area. The visible area allows the user to clearly see and work with data. The obscured area comprises the remaining screen area and makes it difficult or impossible to view data. See col. 1, lines 51-58.

Clearly, Parikh does not disclose at least one publically accessible display and at least one private display in the sense of the present invention. The computer screen in Parikh is not private or publically accessible, but only publically visible.

It is described in col. 3, lines 35-40 of Parikh that the user-selected options may comprise the size of the visible area, the style used for the obscured are, and/or whether to turn the function on/off. It is not clear how this has anything to do with displaying at least a portion of the confidential information at a publically accessible display for a predetermined time period; and concealing the portion of the confidential information displayed at the publically accessible display upon expiration of the predetermined time period or upon a user quest.

Parikh further does not disclose the newly added limitation, namely that the publically accessible display is configured to display the confidential information to only a view from within a predetermined viewing angle and a predetermined distance to the publically accessible display.

The above discussions similarly apply to the rejections over the combination of Sun and Parikh.

Accordingly, the cited references, alone or in combination, fail to disclose or suggest each and every element of Claims 1, 11, and 15. Applicants therefore respectfully submit that Claims 1, 11, and 15 define over the prior art. Furthermore, as each of the remaining claims depends from Claims 1, 11, or 15 while reciting additional features, Applicants further respectfully submit that the remaining claims likewise define over the prior art.

Applicants thus respectfully request that the claim rejections under 35 U.S.C. § 103 be withdrawn.

CONCLUSION

Applicants believe that this application is now in full condition for allowance, which action is respectfully requested. Applicants request that the Examiner call the undersigned if clarification is needed on any matter within this Amendment, or if the]

Examiner believes a telephone interview would expedite the prosecution of the subject application to completion.

Respectfully submitted,

Date: **May 11, 2009**

/Gregory A. Nelson/
Gregory A. Nelson, Registration No. 30,577
Yonghong Chen, Registration No. 56,150
NOVAK DRUCE & QUIGG LLP
Customer No. 40987
525 Okeechobee Boulevard, 15th Floor
West Palm Beach, FL 33401
Telephone: (561) 838-5229